



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/845,221	04/30/2001	Khaja Ahmed	388022001800	4163

7590 01/25/2006
Edward J. Radlo, Esq.
(SONNENSCHN NATH & ROSENTHAL LLP)
6th Floor
685 Market Street
San Francisco, CA 94105

EXAMINER

COLIN, CARL G

ART UNIT	PAPER NUMBER
----------	--------------

2136

DATE MAILED: 01/25/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/845,221

Applicant(s)

AHMED, KHAJA

Examiner

Carl Colin

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 07 November 2005.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-86 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-86 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☒ The proposed drawing correction filed on 07 November 2005 is: a) ☒ approved b) ☐ disapproved by the Examiner.
- If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.
- 14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).
- a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
- 4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/7/2005 has been entered.

Response to Arguments

2. In response to communications filed on 11/7/2005, applicant amends claims 1, 2, 7-12, 15-24, 26, 28-32, 35-50, 52, 55, 57, 68-86. The following claims 1-86 are presented for examination.

2.1 In response to communications filed on 11/7/2005, the amended drawings have been considered and the objection to the drawings has been withdrawn. The objection to the claims has been withdrawn with respect to the amendment.

2.2 Applicant's arguments, pages 20-23, filed on 11/7/2005, with respect to the rejection of claims 1-86 have been fully considered, but they are not fully persuasive as amended. Applicant argues that Orrin does not disclose verifying the trustworthiness of the browser software itself because although Orrin shows multiple signatures, the digital signatures are affixed to the same

entity or to nested versions of the same entity whereas in Applicant's invention, the first signature is affixed to an electronic document and the second signature is affixed to an executable browser software. Examiner respectfully disagrees. First, Orrin discloses or suggests a signature for verifying the trustworthiness of the browser itself (see paragraph 39). Second, the feature of "second signature is affixed to an executable browser software" is not claimed and not disclosed in the specification of Applicant's invention. Upon further consideration, a new ground of rejection is made.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

3.1 **Claims 1-17** are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent Publication US2002/0128940 to **Orrin et al** in view of US Patent 6,292,569 to **Shear et al** (*Applicant IDS*).

Art Unit: 2136

3.2 As per claim 1, **Orrin et al.** discloses a method for verifying the trustworthiness of a executable browser software, said method comprising: transmitting an electronic document requiring a digital signature from a first user computer to a second user computer (page 3, paragraphs 38-39); electronically signing the electronic document by the executable browser software at the second user computer to create a first digital signature, for example (see pages 3-4, paragraphs 0038-0043); including as an attribute of the first digital signature a second digital signature to verify the trustworthiness of the executable browser software itself, the second digital signature verifying the authenticity of at least one component running in an environment of the executable browser software, for example (see pages 3-4, paragraphs 0038-0043 see also page 7); transmitting the signed electronic document from the second user computer to the first user computer, for example (see pages 3-4, paragraphs 0038-0043); authenticating the second digital signature, for example (see pages 3-4, paragraphs 0038-0043). Although **Orrin et al** discloses a second digital signature performed by the browser, **Orrin et al.** does not explicitly state that the second signature is to verify the trustworthiness of the executable browser software itself. **Shear et al** in an analogous art discloses providing secure environment to be implemented between different distribution environment participants, using digital signatures and certificates for verifying the authenticity of the executables and load modules themselves running in the user's environment program (column 4, lines 22-45 and column 5, line 3 through column 4, line 36). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to modify **Orrin et al.** to provide a signature to verify the trustworthiness of the executable browser software and the authenticity of at least one component running in an environment of the executable browser software as taught by **Shear et al.** One of ordinary skill

in the art would have been motivated to do so because as disclosed by **Shear et al** it is important to provide a method to validate the origin of a load module that interacts with other system components operating in the same or different processing environments by using a digital signature or certificate to verify that the load module of the program is intact and was created by a trusted source (column 4, lines 22-45). In addition, a verifying authority can generate different specifications for the load modules and allow other participants to verify that the specifications can be trusted providing a high degree of assurance that the executables and load modules are not subverting the system and the legitimate interest of any participant in a chain the system support (column 5, line 29 through column 6, line 7).

As per claim 2, the combination of **Orrin et al.** and **Shear et al** discloses the limitation of further comprising determining whether the entity that executed the second digital signature is authorized to certify the trustworthiness of the one or more components, for example (see Orrin et al, pages 3-4, paragraphs 0038-0043 and Shear et al, column 12, lines 33-55). Therefore, claim 2 is rejected on the same rationale as the rejection of claim 1.

As per claims 3 and 4, **Orrin et al.** discloses the limitation of wherein the attribute is a signed attribute and an authenticated attribute, for example (see pages 3-4, paragraphs 0038-0043).

As per claims 5 and 6, the combination of **Orrin et al.** and **Shear et al** discloses the limitation of wherein the authenticating comprises verifying the authenticity of the second digital

Art Unit: 2136

signature and wherein the authenticity of the second digital signature is verified using a digital certificate, for example (see pages 3-4, paragraphs 0038-0043 and Shear et al, column 12, lines 33-55). Therefore, these claims are rejected on the same rationale as the rejection of claim 1.

As per claim 7, the combination of **Orrin et al.** and **Shear et al** discloses the limitation of wherein the authenticating comprises comparing a hash of the at least one component running in the executable browser software environment included in the second digital signature to a known-good hash of the at least one component running in the executable browser software environment, for example (see page 5, paragraph 0052). **Orrin et al.** discloses the parties using a web browser, for example (see page 2, paragraph 0023); (Shear et al, column 12, lines 33-55 and column 13, lines 9-35). Therefore, claim 7 is rejected on the same rationale as the rejection of claim 1.

As per claim 8, **Orrin et al.** discloses the limitation of wherein the authenticating is performed by the first user computer, for example (see pages 3-4, paragraphs 0038-0043).

As per claim 9, **Orrin et al.** discloses the limitation of wherein the authenticating is performed by a computer maintained by a financial institution participant, for example (see page 6, paragraph 0070).

As per claim 10, Orrin et al. discloses the limitation of wherein the authenticating is performed by an independent entity that is not a financial institution participant, for example (see page 7, paragraph 0089).

As per claim 11, Orrin et al. discloses the limitation of wherein the authenticating is performed by the second user computer, for example (see pages 3-4, paragraphs 0038-0043).

As per claim 12, the combination of **Orrin et al.** and **Shear et al** discloses that unsigned content can be included in the signature that meets the limitation of wherein an unsigned component running in the browser environment of the second user computer is included as an attribute of the first digital signature, for example (see Orrin et al, page 7, paragraphs 0079-0083).

As per claim 15, Orrin et al. discloses the limitation of wherein a hash of one or more signed browser components running on the second user computer is included as an attribute of the first digital signature, for example (see pages 3-4, paragraphs 0038-0043).

As per claims 13, 16-17, Orrin et al. discloses storing and transferring content on computers comprising of RAM and non-volatile memory, for example (see pages 3-4, paragraphs 0038-0043).

Art Unit: 2136

4. **Claims 18-86** are rejected under 35 U.S.C. 103(a) as being unpatentable by US Patent 6,292,569 to **Shear et al.** (*Applicant IDS*) in view of US Patent Publication US 2005/0114666 to **Sudia**.

As per claims 18, 26, and 41, **Shear et al.** discloses a method of verifying the trustworthiness of a browser comprising: discloses creating set of digital signatures corresponding to a plurality of browser or appliance or protected environment modules at a first point in time (see column 18, line 54 through column 19, line 5 column 8, lines 15-42 and column 13, lines 7 and seq.) that meets the recitation of creating a first set of hashes, the first set of hashes comprising a hash of the browser at a first point in time, and a plurality of hashes corresponding to a plurality of browser components at the first point in time wherein the first set of hashes being a known good set of hashes, for example (see column 10, line 55 through column 11, line 21; column 12, lines 16-55; see abstract); determining the status of the browser running on a computer at a second point in time (column 10, lines 34-55 and column 12, lines 16-55) and discloses creating and verifying the components any time they are presented to another participant that meets the recitation of creating a second set of hashes, the second set of hashes comprising a hash of the browser at a second point in time and a plurality of hashes corresponding to a plurality of browser components at the second point in time (column 4, lines 29-45 column 10, lines 34-55 and column 12, lines 16-55; see also column 21, lines 1-26) verifying the second set of hashes to ensure that each hash was created by a trusted source (see abstract and column 4, lines 29-45) and discloses verifying the digital signatures of the load modules to determine the trustworthiness of the processing environment that meets the recitation

Art Unit: 2136

of comparing the first set of hashes to the second set of hashes to determine the trustworthiness of the processing environment (column 12, , lines 16-55). **Shear et al** discloses another embodiment with different authorities creating and verifying by matching set of hashes at subsequent point in time to determine the trustworthiness of the processing environment (column 18, line 22 through column 19, line 5 see also claims). **Shear et al** does not explicitly disclose comparing the hashes subsequent to the executable browser software module having executed by virtue of having digitally signed an electronic document. **Sudia** in an analogous art teaches verifying that an executable browser software module running in a client environment is trusted invalid trusted by requesting the module to perform a digital signature and comparing hash values to verify that the browser is authentic (page 22, paragraphs 458-466 and page 23, paragraph 475) and further discloses determining whether the status of the browser is bad, invalid, stale, etc. by comparing hash values (see pages 20-21, paragraphs 401-434). Therefore, it would have been obvious to one with ordinary skill in the art at the time the invention was made to modify **Shear et al.** to provide a way for a another party to verify that the user's module is authentic in a transaction by having the browser having executed by virtue of having digitally signed an electronic document and comparing hash values to determine the trustworthiness of the browse as taught by **Sudia**. One of ordinary skill in the art would have been motivated to do so because one of ordinary skill in the art would have recognized some of the advantages disclosed by **Shear et al**, for instance fast multi-party transaction is possible while remained secure wherein the ticket or (cookie) can be served as data record for the server stored on the client (see page 22, paragraphs 462-463, and 467).

Claims 19-23 disclose similar limitations discussed in claim 18 above. **Shear et al** discloses also discloses that the status is unknown if it is determined that a hash was created or not by a trusted source (column 18, line 22 through column 19, line 5 see also claims). Therefore they are rejected on the same rationale as the rejection of claim 18.

As per claims 24-25, **Shear et al.** discloses the limitation of wherein the first set of hashes is maintained by a trusted entity, and further comprising the steps of receiving from a requestor a request to determine the trustworthiness of the browser, the request including the second set of hashes; generating a report about the status of the browser based on a result of the determining step; and transmitting the report to the requestor, for example (see column 10, line 34 through column 11, line 21; column 18, line 22 through column 19, line 5 see also claims; see abstract). Schneier also discloses this limitation as prior art as cited by **Shear et al.** at the end of column 10.

As per claims 27-30, **Shear et al.** discloses similar limitations including the step of determining and verifying hashes by a trusted source as discussed in claim 18. Therefore they are rejected on the same rationale as the rejection of claim 18 and 24.

As per claims 31-34, **Shear et al.** discloses different participants in a financial transaction that meets the recitation buyer and seller. **Shear et al.** further suggests using the invention for on-line financial transaction. Therefore they are rejected on the same rationale as the rejection of claim 24.

Claims 35-40 and 42-49 are similar to the rejected claims 18-34 except for incorporating the claimed method into a system. Therefore, claims 35-49 are rejected on the same rationale as the rejection of claims 18-34.

As per claim 50, claim 50 recites similar limitations as claims 18 and 24 except for incorporating multiple parties. **Shear et al.** substantially teaches the claimed limitations of 18 and 24 as mentioned above and further teaches financial transaction involving multiple parties, for example (see column 10, lines 33 et seq.) including trusted verifier customers and participants. Ginter et al. (for example in column 4, lines 25 et seq.) as mentioned by **Shear et al.** also provides more detailed examples of financial transaction involving multiple parties, which is a well known feature. Therefore it would have been obvious to one with ordinary skill in the art at the time the invention was made to modify **Shear et al.**'s inventive concept to provide the steps performed by each participant. This modification would have been obvious because one skilled in the art would have been motivated by the suggestions provided by **Shear et al** who states that the invention can be implemented into a financial transaction with a verifying authority verifying the browser components of other parties, for example (see abstract and column 10, lines 33 et seq.). **Sudia** discloses performing financial transactions with a plurality of participants including trusted verifier (see pages 24-25 paragraphs 501-508; page 1-2, and claims 1-2); page 13-14, also discloses making inquiries about the status of a party including set of hashes and transmitting and forwarding browser status request to trusted verifier

Art Unit: 2136

and generating response by a trusted verifier (see page 24, paragraphs 483-496). Claim 50 is also rejected on the same rationale as the rejection of claim 18.

Claims 51-59 recite the same limitations as the rejected claims 18-34. Therefore, claims 35-49 are rejected on the same rationale as the rejection of claims 18-34.

As per claims 60-67, Shear et al discloses establishing set of rules (column 15, lines 33-40) and the option of modifying the structure and function of participants and verifying authority, for example (see column 10, lines 33 et seq.).

Claims 68-86 are similar to the rejected claims 50-67 except for incorporating the claimed method into a system. Therefore, claims 68-86 are rejected on the same rationale as the rejection of claims 50-67.

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure as the art discloses security system involving multiple party transactions.

US Patent Publications: US 2002/0124172 Manahan; US 2002/0095579 Yoshiura et al.

US Patents 6,105,012 Chang et al ; 5,958,051 Renaud et al ; 6,157,917 Barber.

Art Unit: 2136

5.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.


Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

cc

Carl Colin

Patent Examiner

January 19, 2006


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100